NAVY MEDICINE
World Class Care…Anytime, Anywhere

DON Application & Database Management System (DADMS)

David Mrazik

BUMED, M6/CIO
Capability Planning and Management Analyst

John Jett

NAVMISSA, Medical FAM/DADMS

DADMS Portfolio Management Analyst

Learning Objectives

- DADMS History / Purpose
- DADMS & DITPR Background
- Roles and Responsibilities
- DADMS and the Governance Process
- DADMS Questionnaire

DADMS History / Purpose

- The Department of the Navy (DON) Application & Database Management System (DADMS) is the Authoritative Data Source for congressionally mandated improvements in management of IT resources. Although initially focused on applications and databases, the success of the system has resulted in its being expanded to include the full range of IT Portfolio Management (PfM).

DADMS History / Purpose (cont.)

- Over 20 DON Functional Area Managers (FAMs), Functional Data Managers (FDM) and others now use DADMS to execute responsibilities in architecture, migration, consolidation, or retirement of IT portfolio resources. The goals are to ensure security, interoperability, and more optimum return on billions of dollars in IT investment. The FAM processes and DADMS enable managers in the DON Secretariat, the Navy, and the Marine Corps to:

  - Adopt systems and applications that best serve DON needs
  - Reduce duplicate functionality
  - Eliminate systems and applications that are vulnerable to attack
  - Better align systems and applications with the Enterprise Architecture
  - Make IT PfM a model for net centric operations

DADMS & DITPR Background

- DITPR and DADMS are key enablers to accomplishing Goal 4 of the DON CIO Campaign Plan – ensure Naval IM/IT investments are efficiently acquired and managed so resources may be recapitalized to support the warfighter. DITPR is the Authoritative Data Source (ADS) for the DoD systems inventory and related information.

- Systems vs. Applications

DADMS & DITPR Background

- Navy Medicine's reporting system as designated by Military Health Systems (MHS) is Defense Health Program Systems Inventory Report Tool (DHP-SIRT) DHP-SIRT.
- DHP-SIRT includes information about MHS systems that support business management decisions, strategic planning, budgeting, information assurance, and privacy reporting required by the Office of the Secretary of Defense (OSD), the Office of Management and Budget (OMB), and Congress.

DADMS & DITPR Background

- DADMS is the ADS for DON system, application, database, and network inventories. It is the planned repository for DON IT Asset Management (ITAM), which will support management of enterprise software licenses and IT procurement. Both DITPR and DADMS support DoD and DON IT Portfolio Management (PfM).

- DADMS and DITPR share a common hardware and software development, test, production infrastructure, and NIPRNET connectivity hosted at AT&T under a GIG waiver. This enables the DoD and DON CIOs to achieve significant cost savings through a shared infrastructure and spiral development. The repositories are an essential component of DoD and DON IM and IT resource management and transformation planning.

DADMS Registration Mandates

- In a 27OCT06 letter, the CNO directed OPNAV N6 take control of the Navy's IT investments to ensure Navy enterprise-wide IT security, interoperability and return on investment. Specific requirements cited
  - Applications – Only Navy Operational Designated Approval Authority (DAA) accredited and FAM 'Approved' or 'Approved – Interim Waiver' (AIW) applications as identified in DADMS will be allowed to be connected to NMCI and/or OCONUS Navy enterprise-network (ONE-NET).
  - Servers, and Networks – Server consolidation/elimination and network elimination will be paced by the current Cyber Condition Zebra (CCZ) network shutdown schedule and integrated under legacy network reduction task force scheme of maneuver, commencing in FY07.
    - Cyber Asset Reduction and Security (CARS) Taskforce Overv...

DADMS Registration Mandates (Cont)

- In a 02 November 2006 BUMED Memo; Subject: Registration of Navy Medicine IT Assets in DADMS
  - It is the longstanding policy of the DON and BUMED that all Navy Medicine IT assets (i.e., Applications, Servers and Networks) be registered in DADMS. DADMS is a web-based system that is the DON's authoritative source for reporting all IT assets.
  - … Navy Medicine commands maintain IT asset information locally, but have only sporadically populated DADMS with this information. As a result, DADMS does not reflect a comprehensive picture of Navy Medicine's current IT assets.

Why should I register my program?

- IM/IT Portfolio Management
  - DoD Instruction 8115.01 (Oct 10, 2005)
    - IT investments shall be managed as portfolio
    - DADMS is a foundational part of Navy Medicine's IT portfolio
    - IT Procurement
      - Software/Software Maintenance can not be procured without DADMS ID
- NAVADMIN 124/05

Why should I register my program?

- DON IT Policy Guidance for FY11
  - "NO FY11 funds… may be obligated for any application that is not registered in DADMS and designated by the appropriate FAM as "Approved" or "AWR"

- Program Certification and Accreditation
  - Navy Network Warfare Command (NETWARCOM) requires DADMS registration for every program or application that is intended to be connected to any Navy network
  - Programs attempting to attain an ATO/IATO must be registered in DADMS
  - Without a DADMS ID, attaining C&A Accreditation is not likely to occur

Roles and Responsibilities

- M6/CIO is the “Information Owner” for all systems/applications\
  - Functional Area Manager (FAM) for Medical
  - Entering/Maintaining the information is shared between M6/CIO and NAVMISSA
    - FAM – Medical
    - ECH II – all other business applications

- System/Application Owners
  - Make sure ALL data related to their system is accurate and up to date
    - DADMS Questionnaire
      - NEW Add
      - UIC Association
      - Equipment

Roles & Responsibilities

SITE
- OCR Reporting Compliance
- Monitoring Software/Hardware

RISO
- Liaison

NAVMISSA
- DADMS Maintenance
- Research and analysis
- Perform legacy application management
- Provide data QA support
- Provide IM/IT portfolio support
- Serves as DADMS SME to BUMED

BUMED
- M6/CIO is the Information Owner
- Policy
- Governance
- Portfolio Management

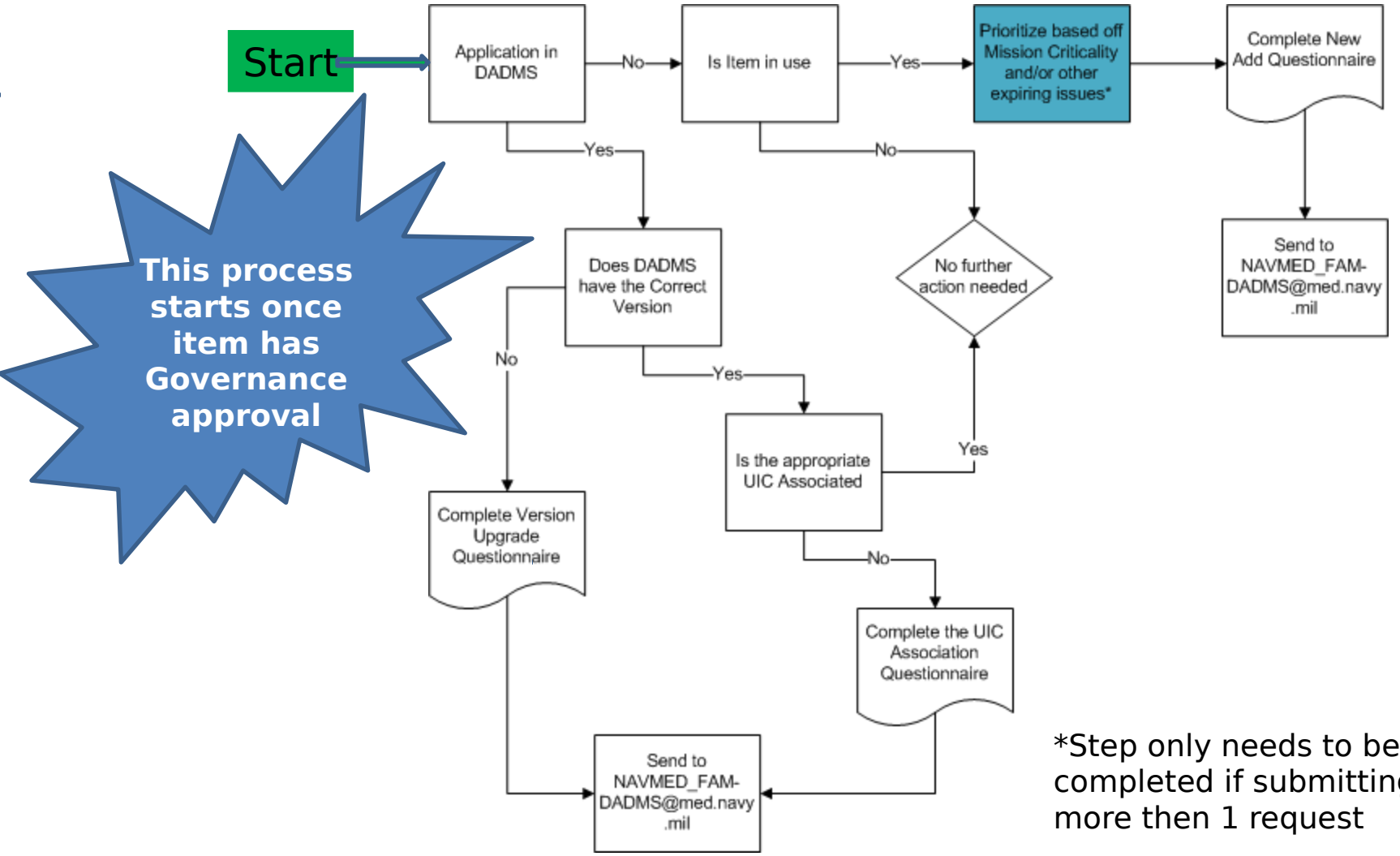
DADMS Medical FAM

Type	Inputs				In-Process	Dispositions				Mid-Term Rat Total
	New Add	Waiver	Question-naire Required	Insuf-Info	Active	Approved	AIW	AWR	Disapproved	
COTS	6	3	0	0	0	60	0	14	80	163
GOTS	5	2	0	0	0	88	0	18	172	285
Unknown	0	0	0	0	0	0	0	0	0	0
TOTAL	11	5	0	0	0	148	0	32	252	448
TOTAL EXPIRED AIW: Now								1	Included in AWR	

FAM Attn Box	Five Day		Allowed Expire		Application Handoff			NMCI Quarantined	ECH II Rec Disapproval	ECH II 50% Reduction	OA Taxonomy	
	Box	Over	In 45 Days	Past Date	IN	OUT	REQ				Mapped	Not Mapped
16	5	5	22	21	0	1	0	0	0	7	178	5

FAM Responsibilities

Decision Tree for what to fill out



*Step only needs to be completed if submitting more then 1 request

DADMS Questionnaire

- STEP ONE – APPLICATION DETAILS
- STEP TWO (a) – UIC STAKEHOLDER ASSOCIATION
  - UIC Questionnaire
- STEP THREE – ASSOCIATED APPLICATION POINTS OF CONTACT
- STEP FOUR – ADD PARENT APPLICATION ASSOCIATION
- STEP FIVE – ASSOCIATED APPLICATION DATABASE
- STEP SIX – CDA/OWNER QUESTIONAIRE

NAVY MEDICINE
World Class Care…Anytime, Anywhere

DADMS BUMED Echelon II

Mid-Term Rationalization Applications Summary

Inputs				In-Process	Dispositions				Total
New Add	Waiver	Questionnaire Required	Ins-Info	Active	Approved	AIW	AWR	Disapproved	Rational-ization
6	174	0	2	1	350	144	327	621	1625
TOTAL EXPIRED AIW: Now							16	Included in AWR	

Echelon II 5 Day					ECH II In-Box	AWR Expire		ECH II 50 % Rec Elimination	NMCI Quarantined	Disapproved Within last 10 days
New Add	Waiver	Ins-Info	Other	OVER		In 45 Days	Past Date			
5	4	2	0	9	341	309	258	45	2	26

NAVY MEDICINE
World Class Care…Anytime, Anywhere

BUMED Echelon II

Functional Area	New/ Rev	Active	Questionnaire Required	Insufficient Info	Waiver	Approved	AIW	AWR	
ACQUISITION	0	0	0	0	0	11	1	0	
CIVILIAN PERSONNEL	0	0	0	0	0	2	0	0	
C2	0	0	0	0	0	0	0	0	
ENTERPRISE SERVICES	0	0	0	9	168	104	113	215	
FINANCIAL MANAGEMENT	0	0	0	0	0	15	3	0	
INFORMATION OPERATIONS	0	0	0	0	18	20	4	8	
INTELLIGENCE	0	0	0	0	0	1	0	0	
LEGAL	0	0	0	0	0	1	0	0	
LOGISTICS	0	0	0	0	5	40	4	0	
MEDICAL	3	0	0	0	2	134	0	27	166
METEOROLOGY, OCEANOGRAPHY, GI&S	0	0	0	0	2	4	3	6	
PERSONNEL MANAGEMENT	0	0	0	0	0	9	0	0	
RRA	0	0	0	0	0	1	0	0	
SCIENTIFIC AND TECHNICAL	0	0	0	0	0	3	14	58	
TEST AND EVALUATION	0	0	0	0	0	0	1	3	
TRAINING AND EDUCATION	0	1	0	1	0	8	1	0	
WEAPONS PLANNING AND CONTROL	0	0	0	0	0	1	0	0	
Total	3	1	0	10	195	354	144	317	1024
Current Date & Time: 05/29/2009 06:19 PM									858

Echelon II Privileges

CODE	PRIVILEGE
APM	Edit Application Step 1 #
UIC	Edit UIC/Waiver Step 2 #
QST	Edit App Questionnaire Steps 3-5 #
CDA	Edit App Questionnaire Step 6 #
ADD	Add Applications to DADMS #
EDN	Edit Echelon II Networks
ADN	Add Echelon II Networks
SGN	Sign for Echelon II
SME	Sign Multiple UICs in Echelon II
ADM	Admin for Echelon II
POC	Echelon II Point of Contact

Select	Group User(s):	Organization (Code):	Privileges										UIC Information	
			APM	UIC	QST	CDA	ADD	EDN	ADN	SGN	SME	ADM	POC	Update	Associated
☐	MRAZIK, DAVID	BUMED	X	X	X	X	X	X	X	X	X	X	X		

BUMED Networks

Search | Echelon II: BUMED [N00018] | Service: DON

SUMMARY | NETWORKS | SERVERS | SRVR APPS | DEVICES | DEV APPS | LABS | DISPLAY ALL

Network Registration and Certification Status

Network Registration Summary

Networks	NTWKs w/o AIS.EXT	Sites	Locations	Devices	Servers	Applications	
						Server	Device
33	30	130	394	4871	2378	887	1

Region Summary

Region	Networks	Sites	Locations	Devices	Servers	Labs
Northeast	8	41	115	1961	902	0
Southeast	7	25	93	686	555	0
Central	5	11	22	241	162	0
Southwest	6	27	57	638	388	0
Northwest	2	5	22	142	64	0
Hawaii	1	5	12	71	44	0
OCONUS	7	16	70	1129	259	0

Other Points to make:

- The AIW Process for Unsupported Applications
- Requesting an LDA Extension
- Getting Networks Allowed on a Record
- Associating a UIC to an Application
- Network Record Management
- Server and Device Management
- Search Capabilities
- Application Waiver Process

- ***The measure of success is not whether you have a tough problem to deal with, but whether it is the same problem you had last year.***

-- John Foster Dulles

Summary

- DADMS (DON Application and Database Management System) is a Web-based, DON application that will manage and track the Navy and Marine Corps software portfolio (https://www.dadms.navy.mil)
- Organized by Functional Area and managed by FAM
- Provides the FAM with the ability to decide disposition and future viability of software by determining if it is allowed for use in the DON

Contact Information

- David Mrazik
  - david.drazik@med.navy.mil
  - 202-762-3132
- John Jett
  - John.jett@med.navy.mil
  - 210-808-0731

Questions

NAVY MEDICINE
World Class Care…Anytime, Anywhere

BACK UP

Systems vs. Applications

SYSTEM:

- Collection of applications or components that are organized for a common purpose.

APPLICATION:

- Program designed to perform a specific function for a user, or another application program.

(i.e.; productivity tools, operating systems, device applications, etc).

DADMS & DITPR Background

Cyber Asset Reduction and Security (CARS) Taskforce Overview

- **CNO (R081315Z Dec 06) directed COMNAVNETWARCOM to establish Task Force (CARS TF) to achieve the following goals:**
  - **By Dec 2008, provide and maintain Navy enterprise IM/IT asset visibility**
  - **By Sept 2010, reduce the Navy's ashore (Secret and below) IT footprint at least 51%**
  - **By Sept 2010, establish and maintain a network protection policy and other mandated security policies on all Navy owned and/or operated ashore NIPR and SIPR networks**
  - **By Sept 2010, eliminate, consolidate and/or migrate capabilities to either:**
    - **Designated enterprise networks (NMCI and ONE-Net), or**
    - **Approved networks that have been excepted to be outside**
    - **Target all other for elimination**

- **DADMS Registration Mandates**

Cyber Asset Reduction and Security (CARS) and What it means for Navy Medicine

- CARS
  - Align to the requirements of the Defense Authorization Act of 2005 and follow the intent of Navy's Cyber Asset Reduction and Security Efforts (CARS)
  - Establish a plan to achieve a 51% overall reduction by 2011
- Savings
  - Fewer servers = lower operating costs
- Security
  - Smaller, more consistent and manageable footprint
- Enterprise Standards
  - Ability to establish Navy Medicine server baselines

  – DADMS Registration Mandates

NAVADMIN 124/05

- NAVADMIN 124/05 established the requirement for Navy networks, servers, and associated network devices to be registered in DADMS.
  - Additionally, it stipulates that Functional Area Manager (FAM) "Approved“ and "Allowed, with Restrictions" (A WR) applications may be linked only to registered servers and that FAM "Disapproved" applications must have their planned termination dates reported in DADMS.
  - No software application may operate on DON Networks unless it is registered in registered and the appropriate FAM designates it as “Approved” ort “AWR”
  - DON IT Policy

FAM Responsibilities

- Overall, FAMs are responsible for:
  - Overseeing the reduction and consolidation of IT applications and databases
  - Authority to direct migration or retirement of applications and databases
  - Development and management of application and database Functional Area portfolios
  - Ensuring that technology strategies are aligned with the business and administration processes and war-fighting strategies of the DON
  - Overseeing migration planning and execution activities.
- FAMs are responsible for identifying and validating system/applications across ALL Navy Medicine Commands and serve as an advocate for the applications in their Functional Area

Functional Areas

OPNAV/SECNAV FUNCTIONAL AREAS
Acquisition
Civilian Personnel
Financial Management
Legal
Medical
Meteorology, Oceanography, and Geospatial Information & Services
Naval Nuclear Propulsion
Precise Time and Astrometry

DADMS Medical FAM

FUNCTIONAL AREAS
Command and Control
Enterprise Services
Information Operations
Intelligence
Logistics
Modeling and Simulation
Personnel Management
Readiness
Resources, Requirements, & Assessments
Scientific and Technical
Test and Evaluation
Training and Education
Weapons Planning and Control

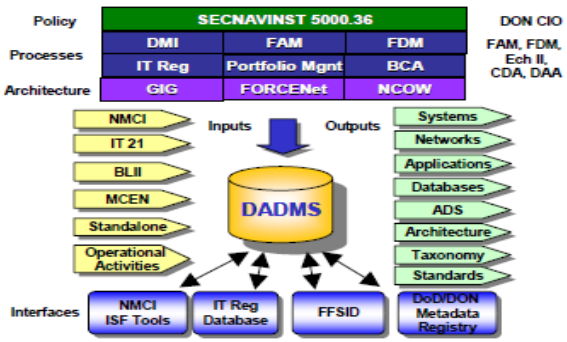
NAVY MEDICINE
World Class Care…Anytime, Anywhere

What Is DADMS?

DADMS is a web-enabled registry of Navy and Marine Corps systems/applications, and their associated data structures. It is the authoritative source for DON IT (including National Security Systems) application and database portfolio management.

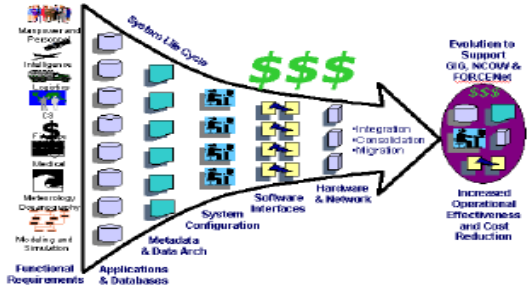
DADMS is an enterprise service that supports DON CIO mission and functions. User organizations include Navy and Marine Corps Functional Area Managers (FAMs), Functional Data Managers (FDMs), Resource Sponsors, Major Claimants, Program Managers, Milestone Decision Authorities (MDA), and operational units.

DADMS Concept of Operations



DADMS Enables the Transformation of Applications and Data into Web-Centric Naval Capabilities

The DON CIO is responsible for ensuring that Department of the Navy Information Management (IM)/ Information Technology (IT) assets are efficiently managed and aligned with warfighter priorities. This is accomplished through the issuance and management of IM/IT policy, development and maintenance of an Investment Management and Implementation Plan, the development and integration of an Enterprise Architecture and Standards, and the protection of information and critical infrastructure.



Establish an Enterprise IT Baseline & Provide Configuration Management that Supports Enterprise Transformation

DON CIO Contact Info:
Mr. Brian Wilczynski
brian.wilczynski@navy.mil
(703) 607-5653
DADMS Helpdesk Contact Info:
dadms@att.com
(703)506-5220
https://www.dadms.navy.mil/

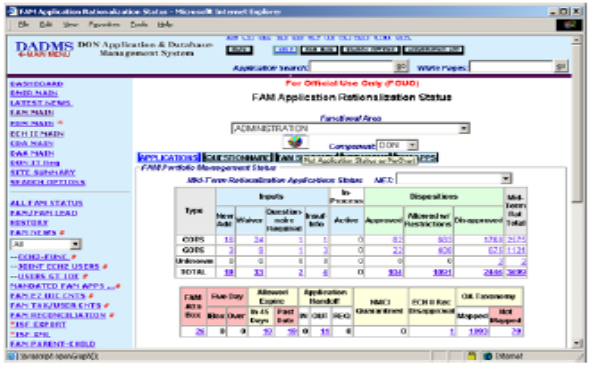
Department of the Navy Application & Database Management System (DADMS)

The Authoritative Data Source (ADS) for DON application and database portfolio management

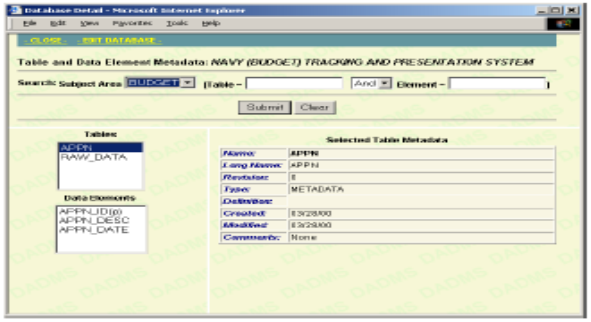
DADMS supports:
- Legacy application, database, and network reduction
- Identification of standard applications, databases, and data elements
- Enterprise Architecture development and maintenance
- Interoperability and Information Assurance assessments

What Is DADMS?

DADMS Supports DON Application Portfolio Management and and Data Management



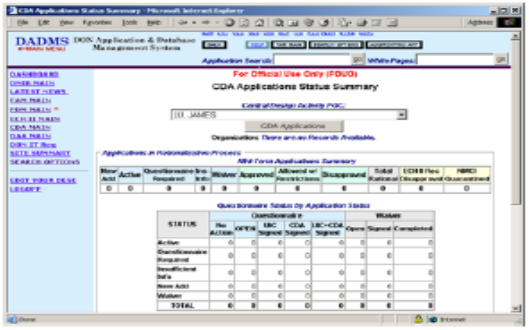
The Functional Area Managers (FAM) use DADMS to execute their responsibilities to direct migration, consolidation, or retirement of applications and databases.



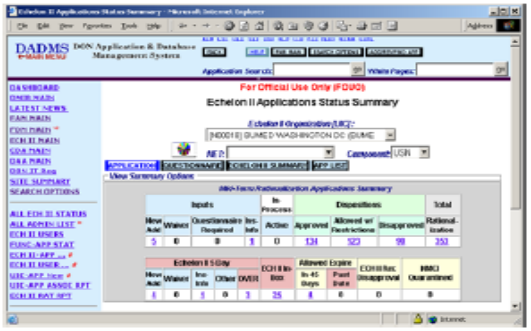
The Functional Data Managers (FDM) use DADMS to assist program managers and other system developers in registering metadata and data exchange formats, developing functional data architectures, and designating authoritative data sources.

Department of The Navy (DON)
Application & Database Management System

Application & Database Portfolio Management	Data Management & Interoperability	Data Architecture & Standards	Information Assurance
• FAM System/Apps Management – DoD IT/NSS Registration – OMB Exhibit 300 – DON Financial & Feeder System Management – FAM App & DB Rationalization – Functional Area Taxonomy – System Reference Documents • Echelon II System/Apps • CDA System/Apps • DAA System/Apps • IT Assessment Support • Task Force Web (TFW) • Information Exchange Requirements	• FDM Data Management – FDM Supported Sys/Apps – Database Registration – Data Source Registration – Data Transfer Format Registration – Database Reference Documents – Sys/Apps Table Names – Sys/Apps DED – Synonyms & Homonyms – Sys/Apps DE to FA Data Model Mapping • Functional Area Data Model • Authoritative Data Sources (ADS) • Data Interoperability Assessment Support • Data Requirements Traceability Analysis	• DOD Data Standards • DON Enterprise Data Architecture – DON Enterprise Data Model – DON Enterprise Data Dictionary • XML Name Space Mapping • DON to DoD Data Standards Mapping • Information Assurance Assessment Support • Standards Documents	• Functionality of Current OCRS Tool • Additional Functionality of NAVFAC IA Tool • Compliance Tracking Functionality of Harris Stat • Sample Areas: • Commands/Organization – To UIC Level • DAA Info – ATO/IATO • IAVA Data • System/Applications Info – POR/Sponsor/Costs – PKI/Firewalls – Certification(s) – Section 508 – CNO Approval – Interfaces • ISSM Information • IA Metrics • FISMA (Federal Information Security Management Act)



The Central Design Authority (CDA) View displays applications by developer/maintainer.



The Echelon II View displays applications by using organization.